Plaintiffs' Response to Google's OSC Response

Redacted Version of Document Sought to be Sealed

BOIES SCHILLER FLEXNER LLP
David Boies (admitted pro hac vice)
333 Main Street
Armonk, NY 10504
Tel: (914) 749-8200
dboies@bsfllp.com

Mark C. Mao, CA Bar No. 236165
Beko Reblitz-Richardson, CA Bar No. 238027
Erika Nyborg-Burch, CA Bar No. 342125
44 Montgomery St., 41st Floor
San Francisco, CA 94104
Tel.: (415) 293-6800
mmao@bsfllp.com
brichardson@bsfllp.com
enyborg-burch@bsfllp.com

James Lee (admitted pro hac vice)
Rossana Baeza (admitted pro hac vice)
100 SE 2nd St., 28th Floor
Miami, FL 33131
Tel.: (305) 539-8400
jlee@bsfllp.com
rbaeza@bsfllp.com

Alison L. Anderson, CA Bar No. 275334
725 S Figueroa St., 31st Floor
Los Angeles, CA 90017
Tel.: (213) 995-5720
alanderson@bsfllp.com

SUSMAN GODFREY L.L.P.
Bill Carmody (admitted pro hac vice)
Shawn J. Rabin (admitted pro hac vice)
Steven M. Shepard (admitted pro hac vice)
Alexander Frawley (admitted pro hac vice)
1301 Avenue of the Americas, 32nd Floor
New York, NY 10019
Tel.: (212) 336-8330
bcarmody@susmangodfrey.com
srabin@susmangodfrey.com
sshepard@susmangodfrey.com
afrawley@susmangodfrey.com

Amanda K. Bonn, CA Bar No. 270891
1900 Avenue of the Stars, Suite 1400
Los Angeles, CA 90067
Tel.: (310) 789-3100
abonn@susmangodfrey.com

MORGAN & MORGAN
John A. Yanchunis (admitted pro hac vice)
Ryan J. McGee (admitted pro hac vice)
201 N. Franklin Street, 7th Floor
Tampa, FL 33602
Tel.: (813) 223-5505
jyanchunis@forthepeople.com
rmcgee@forthepeople.com

Michael F. Ram, CA Bar No. 104805
711 Van Ness Ave, Suite 500
San Francisco, CA 94102
Tel: (415) 358-6913
mram@forthepeople.com

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

CHASOM BROWN, WILLIAM BYATT, JEREMY DAVIS, CHRISTOPHER CASTILLO, and MONIQUE TRUJILLO individually and on behalf of all similarly situated,
 	
       Plaintiffs,
 	
 vs.
 	
 GOOGLE LLC,
       Defendant.
	Case No.: 4:20-cv-03664-YGR-SVK
	
	PLAINTIFFS' RESPONSE TO THE COURT'S ORDER TO SHOW CAUSE (DKT. 784)
	
	The Honorable Susan van Keulen
	Courtroom 6 - 4th Floor
	Date: March 2, 2023
	Time: 10:00 a.m.

TABLE OF CONTENTS

PLAINTIFFS' RESPONSE TO THE COURT'S OSC (DKT. 784) - CASE NO. 4:20-CV-03664-YGR-SVK

1

TABLE OF AUTHORITIES

2

Page(s)

3   **Cases**

27

28

Rules

PLAINTIFFS' RESPONSE TO THE COURT'S OSC (DKT. 784) - CASE NO. 4:20-CV-03664-YGR-SVK

I.   INTRODUCTION

Google's Response demonstrates its repeated and continuing violations of Court orders. Instead of conducting a thorough investigation, Google hid information and conducted a limited review constrained by design to produce a sliver of the discoverable information relevant to this litigation. It has now been twenty-one months, and Google *still* has not done the investigation necessary to identify all relevant and responsive data sources, *still* has not made the representations required by the Court, and as a result new data sources and detection bits are *still* being revealed.

Google's failure to comply with Court orders is demonstrated by Google's revelation *last month* of the "███████████" field, another bit in Google's logging proto that Google used to flag private browsing activity. That field uses a heuristic that ████████████████████ ███████, and it applies not only to Class 1 (Chrome Incognito) but also Class 2 (████████ ███████████). At a minimum, an appropriate investigation early in discovery would have included a search for fields that contain "incognito" in Google's logging protos and server-side source code, followed by an inquiry of all heuristics and methods those fields relied on to log that activity. This would have identified detection fields like "█████████," "is_chrome_incognito," "is_chrome_non_incognito_mode," and "maybe_chrome_incognito," all proto fields that contain the word "incognito." Google's refusal to investigate led to further substantial delay and prejudice, including Google's belated identification of an additional █ logs with Incognito-detection bits. To date, Google still cannot verify that there are no other detection bits or relevant data sources. Nor has Google provided any excuse for why it *waited nearly two months* to disclose this new bit in late December after reportedly discovering it in October. That inexcusable delay proves Google has been acting in bad faith, concealing evidence for strategic purposes—in this instance, waiting for the class certification ruling.

New evidence that Google produced *after* the sanctions order also reveals that key Google employees—including Google's in-house legal counsel for this matter and multiple Google declarants in this case—*did know in 2021* about one or more Incognito-detection bits based on an ongoing internal inquiry that Google was already conducting, before the Court-ordered declaration. This evidence proves Google knowingly and intentionally concealed this discovery.

1

1   Google's "non-accretive" defense to additional sanctions completely misses the point. The

2   Court ordered Google to identify all relevant data sources so that Plaintiffs could understand not

3   only what data Google collected but also what Google services and products were *using* private

4   browsing data, particularly data that Google itself flagged as being private browsing data. That

5   different services and products use the "same (private browsing) data" does not make identification

6   of these additional uses irrelevant, or non-accretive. Google's obstruction prevented Plaintiffs from

7   identifying and conducting fulsome discovery regarding all ways that Google's services and

8   products have used the impermissibly collected private browsing data, which is relevant for

9   purposes of assessing liability and obtaining injunctive relief for the now certified classes.

10   The prejudice to Plaintiffs is especially severe with respect to the newly disclosed private

11   detection methodologies and uses. All three of the previously known bits focused on identifying

12   private browsing activity in Chrome. The prior sanctions order did not cover non-Chrome browsers

13   included in the second certified class. *See* Dkt. 527 at 3 (Google arguing that "the second putative

14   class, comprised of users of *non-Chrome* private browsing modes, is not affected by any of the

15   purported discovery misconduct") (emphasis added). In response to Plaintiffs' interrogatories,

16   Google had represented not only that it "designed" Chrome to prevent detection but that "Google

17   has *no way* of determining how often users use private browsing modes on other browsers." Mao

18   Decl. Ex. 1 at 11 (emphasis added). But Google has in fact sought to make that very determination,

19   using the previously undisclosed "▮▮▮▮▮▮" bit. Plaintiffs are left to only guess what

20   other private browsing-detection methodologies Google concealed. Google's belated disclosure of

21   this field also highlights Google's failure to investigate private browsing detection heuristics and

22   fields used throughout the class period (i.e., 2016 through the present).

23   One of Google's belatedly identified logs (a "▮▮▮" log) further demonstrates Google's

24   prior misrepresentations. Google repeatedly represented that it logs private browsing data separate

25   from GAIA data. The newly identified ▮▮▮ log proves exactly the opposite. More shockingly,

26   the combined information results in exactly the type of user identification that Google and its

27   experts repeatedly attested was not possible. Thompson Decl. ¶ 38. This late disclosure by Google

28   demonstrates another previously unknown and undisclosed way Google used private browsing

data, which undermines one of Google's admittedly "key" defenses—Google's repeated claim that it does not join private data with user's Google Accounts.

Pursuant to the Court's Order to Show Cause (Dkt. 784, "OSC") and subsequent order permitting Plaintiffs to revise the requested relief (Dkt. 826), Plaintiffs respectfully request sanctions to rectify Google's repeated and willful defiance of Court orders.

II.   BACKGROUND

A.   The Court Sanctions Google for Violating Multiple Court Orders.

Google has violated Court order after Court order. On April 30, 2021, the Court ordered Google to "produce all of the named Plaintiffs' data." Dkt. 588 Ex. 1 ("Sanctions Order") at 35 (citing Dkt. 147-1). Google did not comply, so on September 16, 2021, the Court ordered Google to "identify to the Special Master and Plaintiffs all databases and data logs (collectively, 'data sources') that may contain responsive information." Dkt. 273 at 1. On October 27, 2021, Google promised that it "*fully complied* with the Court's various discovery orders, including the April 30 . . . and September 16 orders." Dkt. 312 at 1 (emphasis added).

On November 12, 2021, the Court found that "Google *did not comply* with" its April 30 and September 16 orders. Sanctions Order at 35 (citing Dkts. 147-1, 273, 331) (emphasis added). The Court upheld the Special Master's factual findings "regarding the deficiencies in Google's production" and warned: "Google knows what data it has collected regarding Plaintiffs and putative class members and where that data may be found, therefore Google must produce the information . . . ." Dkt. 331 at 3. The Court ordered Google to "provide a declaration, under penalty of perjury from Google, not counsel, that [] To the best of its knowledge, Google has provided a complete list of data sources that contain information relevant to Plaintiffs' claims." Dkt. 331-1 ¶ 1. Google in response submitted a declaration from Andre Golueke, a Discovery Manager in Google's Legal Department, who swore that Google provided "a complete list of data sources that contain information about Plaintiffs relevant to Plaintiffs' claims." Dkt. 338 ¶ 3.

In May 2022, the Court sanctioned Google for violating all three court orders. Sanctions Order at 35. The Sanctions Order focused on Google's concealment of three Incognito detection bits and ▮ logs identified by Google with those bits: is_chrome_incognito,

1   is_chrome_non_incognito_mode, and maybe_chrome_incognito. *Id.* The Court found that these

2   detection bits are "very clearly relevant to the issues in this litigation." *Id.* at 26. "Mr. Golueke

3   should have been aware of data sources containing the Incognito-detection bits" and his declaration

4   should have included "a complete list of data sources Google has used (and was using at the time)

5   to distinguish Incognito traffic from non-Incognito traffic." *Id.* at 27–28. "[T]he existence and use

6   of three Incognito-detection bits was relevant to both Plaintiffs' claims and Google's defenses"

7   and "Google's unjustified failure to provide information regarding the Incognito-detection bits

8   during discovery was improper and constitutes discovery misconduct." *Id.* at 29.

9   **B.   Google Violates the Sanctions Order.**

10   With its Sanctions Order, the Court also sought to prevent Google from continuing to

11   withhold relevant information responsive to the prior three court orders. During the April 21, 2022

12   sanctions hearing, the Court asked Google's counsel "whether or not there are ***other fields*** that

13   identify incognito traffic . . . that have not yet been identified." 4/21/22 Hrg. Tr. 139:3–4; 16

14   (emphasis added). Google confirmed that "in theory" there could be, but claimed to not know for

15   sure because "it's a difficult thing to do." 4/21/22 Hrg. Tr. 139:9–14. With its Sanctions Order, the

16   Court ordered Google to once and for all come clean: "Google must provide Plaintiffs with a

17   representation in writing no later than May 31, 2022 that other than the logs identified thus far as

18   containing Incognito detection bits, no other such logs exist." Dkt. 588 at 6.

19   On the May 31 deadline, without seeking any extension from the Court, Google sent

20   Plaintiffs a declaration from Martin Sramek informing Plaintiffs that Google would not complete

21   the investigation until June 14 (a week after Plaintiffs' final rebuttal expert reports were due). Dkt.

22   614-3 ¶¶ 4–5. Then, on June 14, Google disclosed for the first time ▮ ***additional logs*** containing

23   the three known Incognito detection bits (Dkt. 614-2 ¶ 4 & at 6–8), but ***without*** providing the

24   Court-ordered representation that no other logs contain Incognito-detection bits.

25   **C.   Plaintiffs Obtain Evidence Proving Google Intentionally Concealed the Incognito Detection Bits and Corresponding Logs.**

26   In July 2022, after the Sanctions Order, Google for the first time produced a non-privileged

27   document demonstrating that Google in 2021 intentionally concealed the Incognito detection bits

28   and corresponding logs. On July 21, 2022, as part of the privilege "re-review" process ordered by

4

the Court, Google produced an internal email thread among Martin Sramek, Bert Leung, Chris Liao, and other Google employees (including Matthew Gubiotti, Google's in-house litigation counsel assigned to supervise this case) discussing Google's use of the X-Client-Data header for Incognito detection. Mao Decl. Ex. 2 at -45. This email thread revealed that no later than September 2021—when Google was reviewing and allegedly nearing completion of custodial document production in this case—Google was investigating how internal employees were using the X-Client-Data header in Google's code, including for Incognito detection. *Id.*

On September 27, 2021, Google program manager Nate Schneider identified Bert Leung and Chris Liao as owners for a "code search result" that mentioned "X-Client-Data." *Id.* While Google never provided those code search results, it appears from the email that the search in September 2021 identified at least the "maybe_chrome_incognito" bit with Mr. Leung and Mr. Liao. Mr. Schneider asked Mr. Leung (along with other Google employees) to confirm "whether your project is reading the X-Client-Data Header from Chrome." *Id.* In early October, Mr. Leung responded that he was using the X-Client-Data header as a "good proxy signal for Incognito" activity (which would have been Mr. Leung's use for "maybe_chrome_incognito") and asked what the "alternatives" might be if he could no longer rely on that heuristic. *Id.* Mr. Schneider engaged none other than Martin Sramek to offer alternatives to the X-Client-Data heuristic. *Id.*

The timing of this email exchange links up with the Court's orders. On November 17, 2021—after more than five weeks of inactivity, but just ***one day before*** Google filed the declaration by Mr. Golueke claiming (falsely) to be identifying all relevant data sources (Dkt. 338)—Messrs. Leung, Liao, and Schneider resurrected this email exchange. Mao Decl. Ex. 2 at -44. Google redacted these subsequent communications as "privileged & confidential" due to "UK ***and US litigation*** and regulatory inquiries," and Mr. Gubiotti was copied on them. *Id.* at -42–44 (emphasis added). These communications raise questions Google has not even tried to answer, including: Why was Mr. Golueke selected to provide the Court-ordered declaration rather than someone like Mr. Sramek, who already knew about the Incognito-detection bits? Who chose Mr. Golueke; was it Mr. Gubiotti? Was Mr. Golueke chosen because he was not on the email thread? Did Mr. Gubiotti review the declaration before it was filed?

PLAINTIFFS' RESPONSE TO THE COURT'S OSC (DKT. 784) - CASE NO. 4:20-CV-03664-YGR-SVK

D.   Plaintiffs Seek Additional Sanctions, and Google Confirms Its Continuing Refusal to Comply with the Sanctions Order.

In August 2022, Plaintiffs moved for additional sanctions, focusing on Google's belated disclosure of the additional ███ logs with Incognito-detection bits and the above email thread. Dkt. 656. In its response, Google declared that it had unilaterally *"reconsider[ed]"* the Sanctions Order to somehow eliminate the requirement that Google conduct a full investigation to identify relevant bits and corresponding logs. Dkt. 695-3 at 3–4. According to Mr. Sramek:

> *I understood the Court's order required me to attest that there are no other data sources at Google in which any field is used by any team to infer Incognito browser state in any form.* To provide such a declaration, multiple months-long investigations would have been required. *However, I understand now that the Court seeks affirmation only for the data sources with the following three fields:* "is chrome incognito";   "is chrome non incognito mode";   and "maybe chrome incognito."

Dkt. 695-4 ¶ 7. Google followed through with this "reconsideration" without seeking clarification from the Court, ignoring the Court's question as to whether there exist "*other fields* that identify incognito traffic" and violating Google's obligations to identify all responsive data sources and represent that no others exist. 4/21/22 Hrg. Tr. 139:3–4; Dkt. 273 at 1; Dkt. 331-1 ¶ 1.

E.   Google's Revealing but Still Deficient Response to the Court's OSC.

On October 27, 2022, this Court ordered Google to show cause "as to why the Court should not find that the logs recently disclosed by Google contain relevant data that should have been identified and produced during discovery and that Google should be sanctioned." Dkt. 784 (the "OSC") at 1. Google's Response was shocking. It confirmed that ██████ log (which contains a private browsing-detection bit) stores *both* private "unauthenticated" data (i.e., signed-out data not explicitly tied to GAIA ID) *and* "authenticated" (i.e., signed-in data explicitly tied to GAIA ID) data. Resp. at 10.

///

///

///

///

///

6

That information contradicts Google's prior representations, including:

- "The most important issue here . . . is that logs are internally segregated by whether you're logged into a Google account or aren't." 4/29/2021 Tr. 16:16-20:2.

- "Google . . . maintain[s] and enforce[s] separation between . . . authenticated logs and . . . unauthenticated logs." Psounis Rep. ¶¶ 45, 47 (Dkt. 659-10).

The truth is that Google stores the data in the same log. This means that if a user signed out of their Google account browses Google in Incognito mode, and then a few minutes later signs into their Google account and continues to browse Google in regular mode: *data on both the ads served responding to signed-out Incognito browsing and the ads served responding to signed-in regular mode browsing are stored together in the same log.*

Time	maybe_chrome_incognito	IP Address	User Agent	URL	GAIA
8:32	True			match.com	
8:34	True			eharmony.com	
8:40	False			nytimes.com	jsmith@gmail.com
8:42	False			store.wsj.com/special-offer/join-now	jsmith@gmail.com
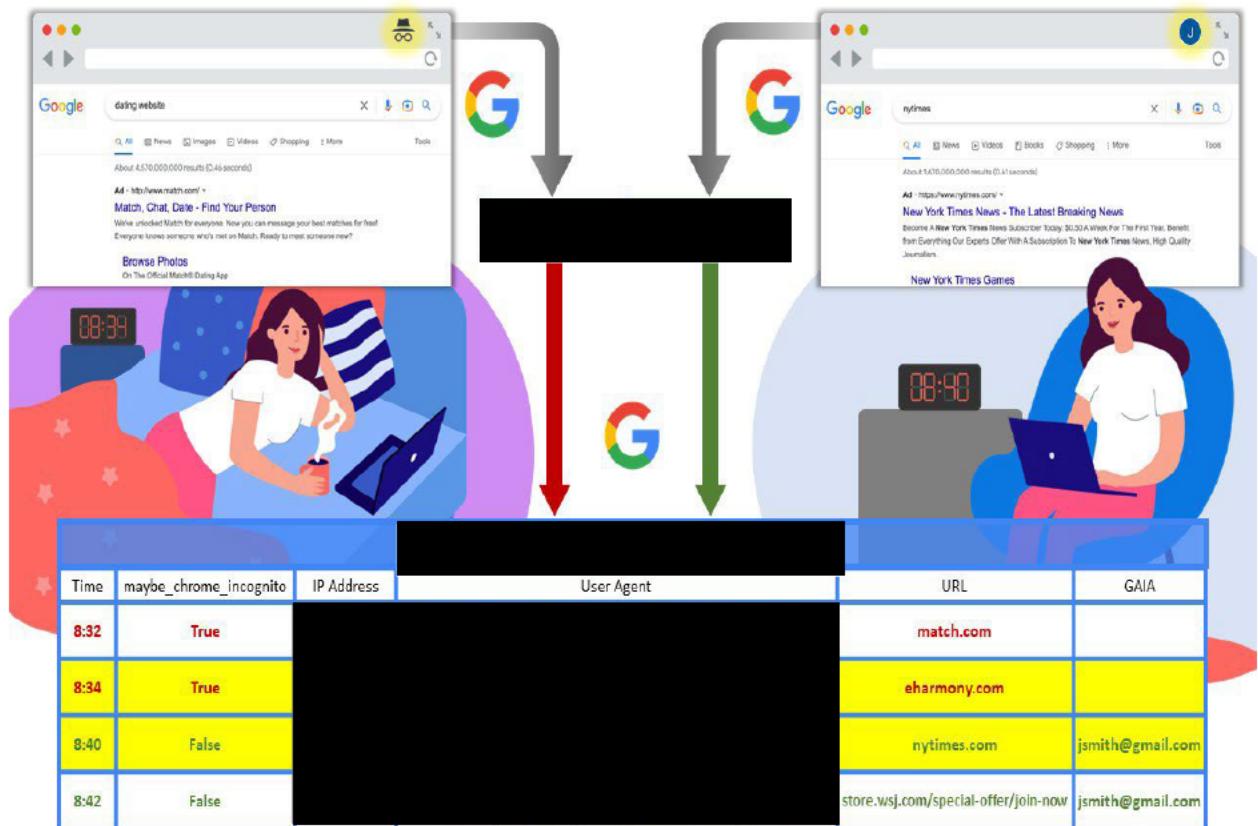
Thompson Decl. ¶ 39. For this log, users browsing in Incognito could easily be identified by matching their IP address and User Agent with those of a known user browsing in regular mode (i.e. jsmith@gmail.com). Simply removing a user's GAIA ID offers little protection when this data is stored together.

Google and its expert Dr. Psounis now tellingly backtrack away from "separation" and instead embrace word games, arguing that this data, which is stored all together in the same log,

7

1   is somehow not "joined." Resp. at 10; Dkt. 798-21 (Psounis Decl.) ¶¶ 2, 9. As a technical matter,

2   Google has fallen far short of its burden to prove what this log does or does not do. *See* Bhatia

3   Decl. ¶¶ 15-25 (identifying deficiencies with the limited source code that Google made available

4   relating to this log)[1]; Thompson Decl. ¶¶ 32, 38 (discussing the import of this log, which identifies

5   users with the same IP address and user-agent string). As a matter of common sense, of course the

6   data is joined. It is in the same log. The same users are also easily identifiable by their IP addresses

7   and User Agent strings. Google's discovery misconduct deprived Plaintiffs of the opportunity to

8   learn about this log and other data sources that likewise combined signed-out private-browsing

9   data and authenticated data containing GAIA IDs.

10   Other revelations in Google's Response include: (1) yet another log with an Incognito

11 detection bit, bringing the total from ▇ to ▇ (Resp. at 5–6); (2) new information regarding how

12 Google uses and monetizes private browsing data (*id.* at 7–8); (3) previously undisclosed logs that

13 populate data in the other logs (*id.* at 9); and (4) a table that could have been used to provide a

14 "longer list [of fields] than what Google was able to produce" during the Special Master process

15 (*id.* at 5 n.2). Notwithstanding all this new information, Google *still* did not provide the Court-

16 ordered attestation that no other logs containing Incognito detection bits exist.[2]

17   **F.   After Filings Its OSC Response, Google Discloses Another Private Browsing
            Detection Bit, Not Limited to Chrome nor The X-Client-Data Header.**

18

19   On December 20, 2022, three weeks *after* filing its Response to the OSC, Google came

    forward with another shocking revelation: a fourth detection bit named "▇▇▇▇▇▇." Mao

20 Decl. Ex. 3. This newly disclosed bit has important implications for this case. Unlike the previously

21 identified bits, this new bit is ***not*** based on the absence of the X-Client-Data header, but rather

22 certain "▇▇▇▇▇▇▇▇▇▇▇▇▇▇▇▇▇▇▇▇▇▇▇▇▇▇▇▇▇▇▇▇

23 ▇▇▇▇▇. *Id.* at 1. Moreover, this bit is relevant not only to Class 1 (Chrome Incognito), but also

24

_____

25 [1] Plaintiffs sought fulsome source code production during discovery, which Google successfully
    opposed. Dkt. 331 at 2. It is improper for Google to now affirmatively rely on source code.

26

    [2] Google also violated the Court's requirement that "Google must provide to Plaintiffs and the
27 Court all facts or data considered by any person proffering evidence in connection with Google's
    opening brief." OSC at 1. The Court made it clear during the prior hearing that Google should do
28 that up front, not after. Hrg. Tr. 10/27/22 6:17–20.

1   Class 2 because it was also used to ███████████████████████████████████████.” *Id.* It was

2   also "created in 2016", the first year of the class period for the certified classes. Dkt. 810 at 1.

3   Google did not provide any list of logs containing that bit, any data schema for those logs, or any

4   information regarding the retention periods and the extent to which Google has during the course

5   of this litigation been deleting data from those logs. *Worse*, Google claims to have discovered this

6   bit in October but waited until December to disclose it. Mao Decl. Ex. 4 at 1. There is no excuse

7   for that delay, but there is an explanation: Google intentionally delayed until after the Court ruled

8   on Plaintiffs' motion for class certification.

9   Not satisfied with concealing this bit until long after the close of discovery, Google quickly

10 moved to "deprecate" it—to destroy evidence. Dkt. 810. Google supported its motion with a

11 declaration from yet another undisclosed employee (Borbala Benko) from a team never before

12 identified (the █████████████), with limited information regarding the bit. Plaintiffs

13 opposed Google's motion and, in doing so, explained why Google's misconduct warrants more

14 severe sanctions, including terminating sanctions. Dkt. 816. The Court granted the parties'

15 stipulated agreement to permit Plaintiffs to seek those more severe sanctions. Dkt. 826.

16 **III.   ARGUMENT**

17   **A.   Google Has Committed New Discovery Violations Not Addressed by the Sanctions Order.**

18   While Google claims that it has committed no "new" violations (Resp. at 14), the evidence

19 proves the opposite. The following details Google's additional violations, none of which were

20 addressed by the Court's prior sanctions order.

21   **1.   Google's Refusal to Provide The Court-Ordered Representation Regarding Additional Incognito-Detection Bits and Heuristics.**

22   In its Response, Google does not even address this violation. Google appears to rest on the

23 representation it made in August 2022—that apart from the █ logs revealed before the Sanctions

24 Order and the █ logs disclosed in June, no other logs exist that contain the *initial three* Incognito-

25 detection bits. Dkt. 695-4 ¶¶ 6–7. As a threshold matter, Google's August representation is false,

26 since Google has now revealed a █ log within its Response.

27   More importantly, Google's self-granted limitation—to just the three previously-identified

28 bits—is not what the Court required, nor does it make any sense given Google's discovery

PLAINTIFFS' RESPONSE TO THE COURT'S OSC (DKT. 784) - CASE NO. 4:20-CV-03664-YGR-SVK

obligations. Google's tracking of private browsing is at the heart of this case. The Court's order (Dkt. 588 at 6) was not limited to just the three **known** Incognito-detection bits, rather it reasonably included **any** Incognito-detection bits or ways Google may infer private browsing. The Order only discussed those three bits by name because those were the only Incognito-detection bits the Court and Plaintiffs were aware of at the time. Nothing in the language of the Court's order restricted Google's representation to logs only containing those three bits.

Nor does Google's interpretation align with the purpose of the Sanctions Order. The Court issued sanctions to cure, in part, Google's violation of two prior Court orders, seeking to identify relevant data sources. Dkt. 273 at 1; Dkt. 331 at 3. The existence of other bits that could be used to infer Incognito, and the logs that contain those fields and bits, is relevant and responsive information. Google's self-serving reinterpretation does not remedy the harm the sanction was designed to cure, and Google's refusal to make that representation is sanctionable.

Google's reinterpretation also ignores the context for the Sanctions Order. The Court made its intentions clear during the sanctions hearing, asking about the existence of any "***other fields*** that identify Incognito traffic?" 4/21/22 Hrg. Tr. 139:3–4 (emphasis added). The Sanctions Order was not issued in a vacuum, and it was within the context of this specific questioning that the Court ordered Google to state whether any additional logs exist—which Google has refused to do. Even Mr. Sramek has declared that he initially (and correctly) "understood the Court's order required me to attest that there are no other data sources at Google in which ***any*** field is used by any team to infer Incognito browser state in any form." Dkt. 695-4 ¶ 7 (emphasis added).

Google's sole excuse for not complying is that Google has unilaterally decided that compliance is too much work. *See* Dkt. 695-4 ¶ 7 ("multiple months-long investigations would have been required"). Notwithstanding the fact that Google appears to have operated under that understanding for nearly three months, and indeed took multiple months after the Court's deadline to submit its representation, this excuse is wholly improper. *Id*. ¶¶ 3, 7. Rather than seek clarification from the Court, Google unilaterally imposed a limitation on the Court's Order, which is a "new" violation that was not remedied by the prior Sanctions Order.

2.   Google's Refusal to Conduct an Appropriate Investigation to Identify All Detection Bits and Data Sources.

Google has also engaged in a "new" violation by refusing to conduct a diligent search to identify all detection signals, heuristics, bits, and data sources. Google's filings reveal that Google limited its code search to references to the X-Client-Data header, which is just one way to identify private browsing data. This was an intentional, self-imposed limitation, and that is in part why Google still cannot state whether other relevant data sources exist.

While searching Google code for references to the X-Client-Data header may allow Google to find logs containing the three Incognito-detection bits previously identified, it would not reveal Google logs containing *other* bits that do not rely on X-Client-Data header to detect Incognito. The insufficiency of Google's restrictive approach is demonstrated by how Google did not identify the new "███████████" bit. Google designed its investigation to miss that bit and any others like it that do not rely on the X-Client-Data header.

By limiting its search in this way, Google has also been able to conceal any methods other than bits which Google has used to infer private browsing traffic, such as adding "client-side signals"—something Plaintiffs have now learned was discussed within Google in 2021, including with Google's in-house litigation counsel, as an alternative means of detecting Incognito. Mao Decl. Ex. 2 at -44; Thompson Decl. ¶ 16 (discussing ability to use client-side signals to detect private browsing). These alternative methods, like the three Incognito-detection bits, "attempt to distinguish" private-browsing traffic and likewise are also "very clearly relevant to the issues in this litigation" and should have been included in Google's investigation. Sanctions Order at 26.

Google also botched the limited investigation it sought to undertake. In response to the Court's OSC, Google apparently wrote a "custom script to query" ██████████ of data from a table called ███████████████. Dkt. 797-6 (Harren Decl.) ¶¶ 7, 11. According to Google's declaration, this table contains "statistical information about fields" in "a random sample of approximately ████████ of ███████ log traffic each day." *Id.* ¶ 8. That table "is not, nor is it designed to be, a comprehensive or fully accurate list of fields in ████████ logs" and does not reveal what fields are contained outside of the ██ of sampled traffic. *Id.*

1   Google's approach suffers from several problems. First, Google limited this review to

2   ████ logs. Google provided no reason for doing so other than attesting that "fields that *might*

3   *be* used for aggregate measurement—such as Incognito-detection bits—are *usually* stored in

4   ████ logs." *Id.* ¶ 5 (emphasis added). Second, Google did not even search fields in ████ of

5   ████ log traffic, instead limiting its review to searching a table containing a random ██ of

6   logged traffic. *Id.* ¶ 8. This is reminiscent of Google's attempt to limit schema production to the

7   largest 100 fields without first disclosing the presence of Incognito-detection bits. Sanctions Order

8   at 37. Third, Google only queried data from logs from "the ████████ days," which would have

9   provided no information on any Incognito-detection bits used outside of this time, with a class

10 period going back to 2016. *Id.* ¶ 11. Finally, and most importantly, without first seeking any

11 guidance from the Court, Google restricted this already limited search to *only* the three Incognito-

12 detection bits disclosed as of June 2022. These Google-imposed limits constitute new violations

13 not addressed by the Court's prior Sanctions Order.

14   **3.   Google's Failure to Timely Disclose ██ Accretive Logs Containing the
                     Three Incognito-Detection Bits.**

15   Google's Response provides no basis to avoid additional sanctions based on these ██

16 additional logs. Google contends that identification of these logs required "extraordinary efforts"

17 (Resp. at 6), but elsewhere clarifies that it only took "three weeks" (Resp. at 4). In any event,

18 nothing precluded Google from conducting this search when the Court first ordered Google to

19 identify responsive data sources in 2021, and Google declared under penalty of perjury that it had

20 done so. Google concedes that if it had used a custom script to identify logs it "would likely have

21 produced a longer list [of responsive logs] than what Google was able to produce earlier using the

22 ████████████ tool." Resp. at 5 fn.2. Long ago, Google could have, and should have, run a

23 custom search for all of the ways Google could infer private browsing traffic.

24   Google has failed to meet its burden to prove that these new logs are "non-accretive" and

25 provide "no new evidence" that should have been disclosed earlier. 10/27/22 Hrg. Tr. 6:11–15;

26 9:10–11. Google's Response suggests, incorrectly, that the only thing that matters is whether those

27 logs contain the same data as other logs previously identified. But how Google *uses* private

28

                                        12

1   browsing data (even if it is the same data) has always been relevant, and accretive. These logs

2   show additional relevant uses, which is relevant both for purposes of liability and injunctive relief.

3   Google's Response also reveals that many of the new ▓ logs—including �███████

4   ██████ logs—either contain data from sources that Google has not previously disclosed, likely with

5   additional data, or contain additional data that reveal their uses. *See* Thompson Decl. ¶¶ 23–29

6   (detailing accretive nature of these additional logs). Most shockingly, one of these logs combines

7   private data with authenticated data, directly undermining Google's repeated assertions that its

8   systems are designed to prevent such joining. *See supra* Section II.E.

9   Discovery regarding these additional logs would have provided a wealth of relevant

10   evidence regarding how Google *uses* private browsing data. As detailed in Plaintiffs' request for

11   additional sanctions (Dkt. 656), Mr. Sramek's declaration demonstrates that Google uses these

12   additional logs to "predict ad revenues," to store "data regarding users' interactions with ads

13   related to third-party exchanges," to create "██████ logs" that "contain information in personal [i.e.,

14   authenticated] logs, which were not previously disclosed by Google," for unspecified "analysis

15   and testing," and for unspecified "test conditions created by Google employees." Dkt. 614-2 ¶¶ 6–

16   10. By failing to identify these additional logs in 2021, Google deprived Plaintiffs of the

17   opportunity to obtain discovery relevant both to liability and the relief sought by Plaintiffs.

18   **4.**   **Google's Failure to Timely Disclose the "████████████████" Field
     And all Logs Containing That Field.**

19

20   Google has also engaged in new violations based on its failure to timely disclose the
     "████████████" bit, and still has not identified the specific logs containing that field. Google

21   did not disclose this field until late December 2022, long after fact and expert discovery, long after

22   the Sanctions Order, after submitting its Response to the OSC, and (most suspiciously) just after

23   the Court ruled on Plaintiffs' motion for class certification. Google now seeks to "deprecate" this

24   bit because, in Google's view, the bit "affect[s] no relevant issue in this case." Dkt. 810 at 3.

25   Google's "no relevant issue" claim is case-in-point for Google's abuse of the discovery

26   process. In violation of blackletter law, Google throughout this litigation unilaterally limited the

27   scope of its discovery obligations without seeking a protective order. Google does not control this

28

1   Court, and Google does not get to "make unilateral decisions about what evidence was relevant."

2   *Leon v. IDX Sys. Corp.*, 464 F.3d 951, 956 (9th Cir. 2006) (quoting district court and affirming

3   terminating sanction). Even after being sanctioned, Google continues to play umpire. The Court

4   warned Google that "the [Incognito] bits are within the scope of discoverable information" and

5   that "***Google was not justified in unilaterally deciding not to provide discovery regarding the***

6   ***bits***." Sanctions Order at 25 (emphasis added). Further, Google admits that "▮▮▮▮▮▮▮▮▮"

7   was "▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮."

8   Mao Decl. Ex. 3 at 1. Thus, like the other detection bits, which were also "specifically designed

9   by Google to attempt to distinguish" Incognito from non-Incognito traffic, the

10 "▮▮▮▮▮▮▮▮" bit is likewise "very clearly relevant to the issues in this litigation." Sanctions

11 Order at 26. This new bit also covers browsers at issue in Class 2, where Google had not otherwise

12 identified any bits used to distinguish private browsing and GAIA data. As with the other detection

13 bits, "▮▮▮▮▮▮▮" is "very clearly relevant" and should have been identified earlier. *Id.*

14   Perhaps just as importantly, Google's belated disclosure of this additional field puts into

15 serious question whether Google disclosed all relevant data sources as of the date of the Court's

16 orders (i.e., 2021 and 2022), or for the entire class period (back to 2016). Google concedes that it

17 was still using "▮▮▮▮▮▮▮▮" as of 2019 for Chrome, and possibly longer for other non-

18 Chrome browsers. If Google had conducted a fulsome search for all relevant data sources for the

19 entire class period, this field would have been identified as well at the onset of the case.

20   **B.   Google's Response Completely Ignores Evidence Demonstrating That
               Google's Discovery Misconduct Was Willful.**

21   The Court should find that Google's discovery misconduct was intentional. Unlike in the

22 prior Sanctions Order, where the Court declined to hold Google acted in bad faith (Sanctions Order

23 at 48), the evidence now proves a pattern of Google intentionally violating Court orders.

24   One aspect of Google's willful misconduct involves its belated disclosure of the

25 "▮▮▮▮▮▮▮" bit. Google's counsel admits that they became aware of that bit in October

26 2022 (*see* Mao Decl. Ex. 4 at 1 (email from Google's counsel containing admission)), which was

27 before Google submitted its Response to the OSC and before the Court issued its certification

28

PLAINTIFFS' RESPONSE TO THE COURT'S OSC (DKT. 784) - CASE NO. 4:20-CV-03664-YGR-SVK

1   ruling. That delayed disclosure was intentional, without any excuse, and it supports a finding of

2   willful discovery misconduct.

3   Seeking to somehow justify its delay, Google seems to suggest that this bit could or should

4   have been known to Plaintiffs—citing a July 18, 2019 Google blog post and July 20, 2019 *Wired*

5   article. Dkt. 810 n. 1 & 3. This is nonsense. Neither of those sources in any way suggests the

6   existence of this detection bit, or what data sources would have been associated with it. The Google

7   blog post (by Barb Palser, who Google never identified as a relevant potential custodian) ***criticizes***

8   how "some sites" (suggesting other sites, not Google) "use an unintended loophole to detect when

9   people are browsing in Incognito Mode" and describes how Google was seeking to block that

10 "circumvention" because "any approach based on private browsing detection undermines the

11 principles of Incognito Mode." Mao Decl. Ex. 5. Similarly, one Google witness in this case

12 testified that the "Incognito detection" at issue with this "loophole" "has always referred to the site

13 you are visiting in Incognito mode, detecting that you are in fact, in Incognito mode." Mao Decl.

14 Ex. 6 [Schuh Tr. 152:4–23]. While Google was publicly criticizing websites for this exact form of

15 Incognito detection, Google was secretly engaged in that same detection, not only for Incognito

16 but other private browsing modes.[3]

17   A finding of willful misconduct is also supported by the de-privileged email thread that

18 Google first produced in July 2022, after the Sanctions Order. Those communications demonstrate

19 that Google's discovery misconduct here is by design. *See* Mao Decl. Ex. 2. Google employees

20 directly involved with this case were aware of one or more of the Incognito-detection bits in 2021,

21 before Google submitted Mr. Golueke's declaration. The investigation addressed in the emails

22 very quickly became relevant to this case, as conceded by the employees who subsequently labeled

23 their (so-called) "privileged" communications as "prepared at the direction of counsel in

24 connection with . . . ***US litigation.***" Ex. 2 at -42-44. (emphasis added). Yet, Mr. Golueke somehow

25 was kept walled away from these employees working on Incognito detection, which included

26

27 [3] The *Wired* article likewise did not disclose Google's internal efforts to detect private browsing
    traffic. Google also cites GOOG-CABR-04331727, but which also only described how "Chrome

28 is closing loopholes that have been used by sites to detect if users are in incognito mode."

15

PLAINTIFFS' RESPONSE TO THE COURT'S OSC (DKT. 784) - CASE NO. 4:20-CV-03664-YGR-SVK

Google's in-house counsel for this case. Google's belated disclosure of the "████ logs" that combine private browsing and GAIA data further shows a pattern of willful misconduct. The ████ log shows Google doing exactly that, with private browsing data stored alongside GAIA data in this log. Thompson Decl. ¶ 37.

C.   Google's Additional Discovery Misconduct Has Prejudiced Plaintiffs In Ways Not Addressed By the Court's Prior Sanctions Order Against Google.

1.   Fact Discovery

Google's misconduct prejudiced Plaintiffs by depriving Plaintiffs of relevant discovery. Like the ██ logs addressed in the Sanctions Order, the ██ new logs (along with the unknown number of logs containing the "████████" field and any other detection bits and heuristics) "all track incognito traffic and therefore plainly contain information relevant to Plaintiffs' claims." Sanctions Order at 36. There was no discovery provided for these additional logs (e.g., the new ████ log that combined "logged in" and "logged out" data) and the new "████████" bit. Neither the Court nor the Plaintiffs know what other detection heuristics or fields have been withheld by Google. The additional discovery could have provided even more support for Plaintiffs' claims and requested relief, beyond just the existence of these additional logs and fields. The entire "course of discovery may have been different, more focused, or focused on different issues had Google complied with its discovery obligations" and provided this discovery when required by the Court's prior orders. *Id*. at 31.

The prejudice is especially pronounced for the new ████ log that combines both private and non-private browsing data. This log's existence contradicts Google's repeated assertions that it does not join private browsing data with "authenticated" data. *See supra* Section II.E. Had this log been disclosed, Plaintiffs would have sought additional discovery about this log and others like it, including through document productions and questioning witnesses. But because of Google's willful misconduct, Plaintiffs will never know the truth.

The same is true with respect to the "████████" bit, and any other bits and fields— and any logs containing them—that Google still has not identified. That "████████" bit verifies, for the first time, what Plaintiffs have long suspected: Google's identification and tracking

1 of private browsing was not limited to Chrome Incognito mode, nor the X-Client-Data header

2 heuristic. There are likely even more bits based on more heuristics that Plaintiffs will never learn

3 about because of Google's misconduct. Google's failure to provide that discovery earlier deprived

4 Plaintiffs of the opportunity to assess and litigate Google's full liability on the merits, versus

5 Google's demonstrably false representations. Plaintiffs never obtained documents, issued

6 interrogatories, or deposed key witnesses (including Borbala Benko, the declarant selected by

7 Google) about the " ███████████ " bit, because Plaintiffs simply did not know the bit existed.

8   2.   **Expert Discovery**

9   Google's additional discovery misconduct also prejudiced Plaintiffs with respect to expert

10 discovery. Plaintiffs' technical expert sought to assess the various ways in which Google stores

11 and uses private browsing data. The additional logs containing the three initial Incognito-detection

12 bits, the additional " ███████████ " and corresponding logs, and any other detection bits and

13 corresponding logs are all core to that expert analysis. Had Plaintiffs had this information earlier,

14 Plaintiffs could have requested the algorithm Google uses to track Incognito using APIs, or run

15 tests on how accurately " ███████████ " detects private browsing. The belatedly identified

16 ████ log directly refutes Google's prior attestations about the separation of authenticated and

17 unauthenticated data. Rounds of unnecessary expert discovery were wasted on a defense refuted

18 by Google's own use of data.

19   3.   **Injunctive Relief**

20   Google's misconduct has deprived Plaintiffs of information relevant to the injunctive relief

21 sought on behalf of the two certified classes, in ways unaddressed by the Sanctions Order. As

22 stated in the Court's certification ruling, Plaintiffs seek injunctive relief in the form of "important

23 changes to reflect transparency in the system." Dkt. 803 at 34. The relief would:

24   (1) preclude Google from collecting further private browsing information; (2)
        require Google to delete the private browsing information that it previously
25   collected and is currently storing; (3) require Google to remove any services that
        were developed or improved with the private browsing information; and (4)
26   appointment of an independent third-party to verify that the injunctive relief has
        been implemented.

27

28

1   *Id.* at 33–34. Google's claim that it has already "acknowledged" that it "leverages private browsing

2   data" for various purposes overlooks Plaintiffs' prejudice. Resp. at 16. Without full discovery on

3   how Google collects, stores, and uses private browsing information, Plaintiffs are prejudiced in

4   their ability to fashion and obtain full injunctive relief. Plaintiffs need to be aware of something

5   before they can ask the Court to order Google to remove it. Plaintiffs also face obstacles in terms

6   of ensuring that Google removes all services and products developed or improved with private

7   browsing information.[4]

4.   Preservation

9   Because Google did not timely disclose the additional ▮ logs, the "▮▮▮▮▮▮▮" bit

10   and corresponding logs, or logs associated with any other detection bits, none of these additional

11   logs were subject to the preservation briefing and the Court's rulings. The Special Master made

12   his proposal (Dkt. 524), the parties submitted briefing (Dkts. 544, 546), the Court issued its order

13   (Dkt. 587), and Google sought to clarify that order (Dkt. 591), all before Google revealed the

14   additional logs, bit, and deficiencies. Despite "plainly contain[ing] information relevant to

15   Plaintiffs' claims," these logs were neither included in this process nor protected by this procedure,

16   and Google has been able to continue purging relevant data. Sanctions Order at 36. Notably,

17   Plaintiffs sought to meet and confer with Google regarding preservation in connection with the

18   additional logs, and Google refused. Dkt. 650.

D.   Plaintiffs Appropriately Seek Additional Sanctions.

20   Google's Response confirms the importance of awarding additional relief based on

21   Google's additional misconduct, to address the additional prejudice to Plaintiffs. Plaintiffs—once

22   again—find themselves in the position of having to update their sanctions request due to Google's

23   everchanging disclosures and still further misconduct.[5] Plaintiffs continue to seek preclusion and

24

25   _____

26   [4] There is precedence for destroying algorithms and services created using ill-gotten data. *See United States v. Kurbo Inc., et al.*, 22-cv-00946-TSH (N.D. Cal. Mar. 3, 2022) (ordering deletion of models and algorithms made with data alleged to be improperly obtained); *see also In the Matter of Everalbum, Inc., et al.*, FTC Docket No. C-4743 (May 6, 2021) (same).

27   [5] Including additional relief is consistent with the parties' stipulation and the Court's resulting

28   order (Dkt. 826) permitting Plaintiffs to expand the requested relief without an additional OSC.

1   monetary sanctions, but also more severe sanctions given Google's intentional misconduct, as

2   confirmed by recently disclosed evidence.

3   **1.   Terminating Sanctions Are Warranted.**

4   After 21 months of Google's intentional violation of discovery orders, Plaintiffs ask that

5   the Court now issue terminating sanctions. Default judgment and terminating sanctions are

6   "warranted in instances wherein a party has intentionally hidden or destroyed evidence to the

7   extent it severely undermines the Court's ability to render a judgment based on the evidence and

8   threatens the 'orderly administration of justice.'" *OmniGen Research. v. Yongqiang Wang*, 321

9   F.R.D. 367, 371 (D. Or. 2017) (quoting *Leon v. IDX Sys. Corp.*, 464 F.3d 951, 958 (9th Cir. 2006)).

10   This Court has the authority to impose terminating sanctions under: (1) Federal Rule of Civil

11   Procedure 37(b)(2) (for disobeying discovery orders); (2) Rule 37(c)(1)(C) (for failing to provide

12   information or identify witnesses); (3) Rule 37(e) (for spoliation of electronic evidence); and (4)

13   the Court's inherent authority (for abusive litigation practices). *Id.*; *see also CrossFit, Inc. v. Nat'l*

14   *Strength & Conditioning Ass'n*, No. 14-CV-1191 JLS (KSC), 2019 WL 6527951 (S.D. Cal. Dec.

15   4, 2019). To award terminating sanctions, the court must find that the disobedient party's

16   noncompliance is "due to willfulness, fault, or bad faith." *Computer Task Grp., Inc. v. Brotby*, 364

17   F.3d 1112, 1115 (9th Cir. 2004) (quoting *Payne v. Exxon Corp.*, 121 F.3d 503, 507 (9th Cir. 1997))

18   (marks omitted). But "disobedient conduct not shown to be outside the control of the litigant is all

19   that is required to demonstrate willfulness, bad faith, or fault." *K. P. v. Santa Clara Cnty. Off. of*

20   *Educ.*, No. 5:15-CV-01512-EJD, 2016 WL 5930641, at *3 (N.D. Cal. Oct. 12, 2016) (quoting

21   *Henry v. Gill Indus., Inc.*, 983 F.2d 943, 948 (9th Cir. 1993)). The record is replete with evidence

22   that Google has intentionally disobeyed Court order after Court order, and is continuing to violate

23   the Court's orders. *See supra* Sections II.C, E, II.A.2, III.B.

24   Courts apply a five-factor test for imposing terminating sanctions: "(1) the public's interest

25   in expeditious resolution of litigation; (2) the court's need to manage its docket; (3) the risk of

26   prejudice to the party seeking sanctions; (4) the public policy favoring the disposition of cases on

27   their merits; and (5) the availability of less drastic sanctions." *Connecticut Gen. Life Ins. Co. v.*

28   *New Images of Beverly Hills*, 482 F.3d 1091, 1096 (9th Cir. 2007) (marks omitted). "[T]he most

1   critical factor…. is whether the discovery violations threaten to interfere with the rightful decision

2   of the case." *Id*. at 1097.

3   These factors weigh in favor of terminating sanctions. First, and most importantly,

4   Google's discovery violations have made it impossible to discover the full truth about Google's

5   collection, storage, and use of private browsing data. These matters go to the heart of this case,

6   thus weighing heavily in favor of terminating sanctions. *See Valley Eng'rs Inc. v. Elec. Eng'g Co.*,

7   158 F.3d 1051, 1057 (9th Cir. 1998) ("[d]ismissal is appropriate where a 'pattern of deception and

8   discovery abuse made it impossible' for the district court to conduct a trial 'with any reasonable

9   assurance that the truth would be available.'" (quoting *Anheuser-Busch, Inc. v. Nat. Beverage*

10   *Distributors*, 69 F.3d 337, 352 (9th Cir. 1995)). Google's misconduct has deprived Plaintiffs of

11   key evidence on what private browsing data is captured, how it is stored, and how Google uses it.

12   Proceeding to summary judgment and trial without this information is highly prejudicial to

13   Plaintiffs. *See Anheuser-Busch, Inc.*, 69 F.3d at 353–54 ("defendant suffers prejudice if the

14   plaintiff's actions impair the defendant's ability to go to trial or threaten or interfere with the

15   rightful decision of the case.").[6]

16   The remaining factors together also weigh in favor of Plaintiffs. For factors one and two,

17   Google was ordered to produce this evidence in April 2021, and nearly two years later still has not

18   complied. *See Valley Engineers Inc.*, 158 F.3d at 1059 (affirming terminating sanctions where

19   lawyers violated court orders requiring document production for more than two years). While

20   factor four weighs against terminating sanctions, Google's pattern of repeatedly violating Court

21   orders outweighs this consideration. *See Reddy v. Gilbert Med. Transcription Serv., Inc.*, 467 F.

22   App'x 622, 624 (9th Cir. 2012) ("[t]he district court did not abuse its discretion by imposing

23   terminating sanctions under Fed. R. Civ. P. 37(b)(2)" based on "willful and repeated violations of

24

25   [6] Plaintiffs were also prejudiced by not having this evidence protected by the Court's preservation
     orders. Google was aware this evidence was pertinent to this litigation since at least September
26   2021, making any loss of this evidence willful and, therefore, weighs in favor of terminating
     sanctions. *See CrossFit, Inc.*, 2019 WL 6527951 at *10 (S.D. Cal. Dec. 4, 2019) (issuing
27   terminating sanctions reasoning "[a] party's destruction of evidence can be considered willful or
     in bad faith when the party had notice that the evidence was potentially relevant to litigation before
28   it was destroyed." (marks omitted)).

PLAINTIFFS' RESPONSE TO THE COURT'S OSC (DKT. 784) - CASE NO. 4:20-CV-03664-YGR-SVK

the court's discovery orders"); *see also Wyle v. R.J. Reynolds Indus., Inc.*, 709 F.2d 585, 590 (9th Cir. 1983) (affirming district court's issuance of terminating sanctions where "[s]ufficient evidence support[ed] the district court's finding that [the plaintiff], through [its counsel], willfully failed to comply with discovery orders"). Finally, Google's persistent refusal to provide required discovery here makes less drastic sanctions infeasible. *See Anheuser-Busch, Inc.*, 69 F.3d at 352 ("[i]t is appropriate to reject lesser sanctions where the court anticipates continued deceptive misconduct."); *see also Valley Engineers Inc.*, 158 F.3d at 1058 ("no point to a lawsuit, if it merely applies law to lies.").

2. Alternatively, Additional Preclusion Sanctions Are Warranted.

i) *Preclusion in the form of Court findings.*

Because Google has repeatedly and continuously withheld discovery that is relevant to proving certain elements of Plaintiffs' claims, if the Court declines to award terminating sanctions, Plaintiffs request that the Court make certain findings for purposes of summary judgment and through the ultimate disposition of this case. *See* Fed. R. Civ. P. 37(b)(2)(A)(i) (permitting the Court to "direct[] that the matters embraced in the order or other designated facts be taken as established for purposes of the action"); Fed. R. Civ. P. 37(c)(1)(C) (failing to provide information or identify a witness); Fed. R. Civ. P. 37(e)(1) (failing to preserve ESI); *Guifu Li v. A Perfect Day Franchise, Inc*, 281 F.R.D. 373, 396 (N.D. Cal. 2012) (court's inherent authority). Based on Google's additional misconduct, the full scope of which will never be known, Plaintiffs request that the Court make the following findings, modified from what Plaintiffs initially proposed in their August motion seeking additional sanctions:

1. Throughout the class period, Google used multiple processes to identify Plaintiffs' and class members' private browsing activities.
2. Throughout the class period, Google used multiple processes to detect private browsing activities in at least Chrome, Safari, and Edge.
3. Throughout the class period, Google systematically intercepted, collected, stored, and used Plaintiffs' and class members' private browsing information.
4. Throughout the class period, Google read and learned the contents or meaning of Plaintiffs' and class members' private browsing communications.
5. Throughout the class period, Google took, copied, and made use of Plaintiffs' and class members' private browsing data.

6. Throughout the class period, Google readily and systematically mixed private browsing data with the other data it stores.

7. Throughout the class period, Google's use of browsing data to develop or improve any products, services, or algorithms presumptively included private browsing data.

8. Throughout the class period, Google's conduct in terms of collecting, storing, and using Plaintiffs' and class members' private browsing data was highly offensive.

9. In response to multiple court orders, Google withheld relevant information regarding its collection, storage, and use of private browsing data.

These requested sanctions are also listed in the Mao Declaration. *See* Mao Decl. Ex. 7. Such sanctions are warranted because Google's delays have deprived Plaintiffs of "a meaningful opportunity" to "comprehend" how collects, stores, and uses private browsing data. *Apple Inc. v. Samsung Elecs. Co.*, No. C 11-1846 LHK PSG, 2012 WL 1595784, at *3 (N.D. Cal. May 4, 2012).

ii)   *Preclusion regarding certain Google arguments.*

Based on Google's discovery misconduct, this Court may "prohibit[] [Google] from supporting or opposing designated claims or defenses, or from introducing designated matters in evidence." Fed. R. Civ. P. 37(b)(2)(A)(ii); *see also* Fed. R. Civ. P. 37(c)(1)(C); Fed. R. Civ. P. 37(e)(1); *Guifu Li*, 281 F.R.D. at 396 (court's inherent authority). "[I]t is entirely reasonable to sanction [Google's] defiance of the [numerous discovery] Order[s] by precluding [it] from presenting evidence on [issues for which Google] ha[s] not provided timely and complete discovery." *Sas v. Sawabeh Info. Servs.*, No. CV114147MMMMANX, 2015 WL 12711646, at *11 (C.D. Cal. Feb. 6, 2015). Plaintiffs request that the Court now preclude Google from making the following arguments:

1. Google is precluded from arguing that it has no way of determining how often users use private browsing modes.

2. Google is precluded from arguing that it does not join private browsing data to authenticated data.

3. Google is precluded from arguing that its data sources, including those sources for authenticated data, does not include private browsing data.

4. Google is precluded from arguing that it does not use private browsing data to "perform analysis and modeling to predict ad revenues."

5. Google is precluded from arguing that it does not use private browsing data for "ads related to third-party exchanges."

22

PLAINTIFFS' RESPONSE TO THE COURT'S OSC (DKT. 784) - CASE NO. 4:20-CV-03664-YGR-SVK

6.   Google is precluded from arguing that it has not made private browsing data available for other business purposes.

This limited relief, which is crafted to preclude Google from contesting facts that are made clear from Google's submissions. *See* Mao Decl. Ex. 7. Google's failure to comply with Court orders has prevented Plaintiffs' efforts to fully understand these issues. It is now "appropriate, based on these failures, to preclude [Google] from introducing further facts or evidence in response to these issues" to prevent Google from exploiting the evidentiary gaps it has created. *Lanier v. San Joaquin Valley Offs. Ass'n*, No. 1:14-CV-01938-EPG, 2016 WL 4764669, at *8 (E.D. Cal. Sept. 12, 2016); *see also Shanghai Weiyi Int'l Trade Co. v. Focus 2000 Corp.*, No. 15CV3533CMBCM, 2017 WL 2840279, at *11 (S.D.N.Y. June 27, 2017) (where, as here, "the discovery misconduct has deprived the opposing party of key evidence needed to litigate a contested issue, an order prohibiting the disobedient party from contesting that issue . . . is. . . appropriate.").

iii)   Witness and testimony preclusion.

Plaintiffs further request the Court preclude Google from relying for any purpose on the testimony of the numerous undisclosed Google employees now relied on for its Response and other post-discovery filings, where none of these names appeared in the list of 220 employees Google disclosed earlier: Martin Sramek, Matt Harren, Borbala Benko, Maciej Kuzniar, Eugene Lee, Xianzhi Liu, Eric Maki, and Vasily Panferov. *See* Rule 37(c)(1); Rule 37(e)(1); *Guifu Li*, 281 FRD at 396 (Court's inherent authority). Under Rule 37(c)(1), the Court previously precluded Google from offering or relying on any testimony from four Google engineers. Sanctions Order at 40. With respect to these eight additional Google employees, Google also "violated Rule 26(e) when it failed to disclose [them] in response to Plaintiffs' interrogatory asking Google to identify employees 'with responsibility for or knowledge of . . . Google's collection of and use of data in connection with users' activity while in a private browsing mode.'" Sanctions Order at 55; Dkt. 429-15 (interrogatory response); Dkt. 429-11 (list of over 200 Google employees).

The evidence disproves Google's claim that Mr. Sramek's "knowledge became only relevant as a result of the Court's [sanctions] Order." Resp. at 21. Mr. Sramek was involved with

1   Google's Fall 2021 X-Client-Data header investigation, which involved Bert Leung and Chris Liao

2   and their work on Incognito detection. Mao Decl. Ex. 2 at -45. Mr. Sramek has also admitted, in

3   his May Declaration, that he was "aware of" the three initially disclosed bits "[b]ased on [his]

4   experience" "responding to requests by Googlers related to inferring Incognito mode on Chrome."

5   Dkt. 614-3 ¶ 4. There is no excuse for Google's failure to disclose him, and there is only one

6   explanation: Google was intentionally concealing its private-browsing detection bits.

7   Google's failure to disclose Vasily Panferov is also particularly egregious since he has

8   "personal knowledge" of the ████ log that joins unauthenticated data with authenticated data.

9   Dkt. 797-19. Moreover, Mr. Panferov tellingly does not disclaim prior knowledge of private-

10 browsing detection bits. The same is true for Maciej Kuzniar. Dkt. 797-10. As for the other

11 undisclosed witnesses, they questionably have knowledge about how private browsing data is

12 being used. If Google had complied with the Court's various orders, they would have been timely

13 disclosed and possibly become document custodians and deponents. Google's failure to do so was

14 neither substantially justified nor harmless. Having failed to disclose them earlier, Google should

15 not be permitted to rely on additional declarations or testimony from these individuals.

16   **3.   Additional Monetary Sanctions Are Warranted.**

17   Plaintiffs respectfully request that the Court order Google to once again pay Plaintiffs'

18 attorneys' fees and expenses, including expert fees, incurred with their requests for additional

19 sanctions. Dkt. 593-3 at 42.[7] Plaintiffs incurred those fees and costs only as a result of Google's

20 discovery misconduct, and the Court again has the power to award those fees and costs to Plaintiffs.

21 *See* Fed. R. Civ. P. 37(b)(2)(A)(ii); Fed. R. Civ. P. 37(c)(1)(C); Fed. R. Civ. P. 37(e)(1); *Guifu Li*

22 281 F.R.D. at 396 (court's inherent authority). Plaintiffs also respectfully renew their request for

23 Google to reimburse them for all fees paid to the Special Master. Dkt. 430 at 22–23. Plaintiffs also

24 ask that Google be ordered to pay a portion of Plaintiffs' attorneys' fees and expenses, including

25

26 _____

27 [7] Google's Response primarily relies on the defense that the new logs are non-accretive, stating the additional logs "provide no additional information that would have obviated the special master process (or a portion of it)." Resp. at 24. Had Google provided this information during discovery,

28 it could have streamlined that costly process. Thompson Decl. ¶¶ 9–22.

PLAINTIFFS' RESPONSE TO THE COURT'S OSC (DKT. 784) - CASE NO. 4:20-CV-03664-YGR-SVK

1   expert fees, incurred within the Special Master process more broadly due to Google's obstruction,

2   which made the process longer and more expensive than necessary.[8]

3   **IV.   CONCLUSION**

4   Plaintiffs respectfully request that the Court direct the parties to submit findings of fact and

5   conclusions of law in advance of the March 2, 2023 hearing, and impose the sanctions discussed

6   above.

7
    Dated: January 20, 2023   BOIES SCHILLER FLEXNER LLP
8

9
                                                    By */s/ Mark C. Mao*
10

11
                                                    Mark C. Mao (CA Bar No. 236165)
12   mmao@bsfllp.com
                                                    Beko Reblitz-Richardson (CA Bar No. 238027)
13   brichardson@bsfllp.com
                                                    Erika Nyborg-Burch (CA Bar No. 342125)
14   enyborg-burch@bsfllp.com
                                                    BOIES SCHILLER FLEXNER LLP
15   44 Montgomery Street, 41st Floor
                                                    San Francisco, CA 94104
16   Telephone: (415) 293 6858
                                                    Facsimile (415) 999 9695
17

18   David Boies (*pro hac vice*)
                                                    dboies@bsfllp.com
19   BOIES SCHILLER FLEXNER LLP
                                                    333 Main Street
20   Armonk, NY 10504
                                                    Tel: (914) 749-8200
21

22

23

24

    _____

25 [8] To streamline these proceedings, Plaintiffs respectfully request the Court defer ruling on their
    request for additional jury instructions so that the parties may first obtain guidance from the Court
26 regarding how this case may proceed (be it a jury or bench trial). Jury instructions also may be
    relevant at a later date depending on how the Ninth Circuit rules on Plaintiffs' Rule 23(f) petition.
27 If the Court does not wish to defer that ruling, then Plaintiffs would seek the requested jury
    instructions as well as additional instructions tied to "███████████," that Google
28 systematically joins authenticated and unauthenticated data, and Google's refusal to search for and
    identify all detection bits.

James W. Lee (*pro hac vice*)
jlee@bsfllp.com
Rossana Baeza (*pro hac vice*)
rbaeza@bsfllp.com
BOIES SCHILLER FLEXNER LLP
100 SE 2nd Street, Suite 2800
Miami, FL 33130
Telephone: (305) 539-8400
Facsimile: (305) 539-1304

Amanda Bonn (CA Bar No. 270891)
abonn@susmangodfrey.com
SUSMAN GODFREY L.L.P.
1900 Avenue of the Stars, Suite 1400
Los Angeles, CA 90067
Telephone: (310) 789-3100

Bill Carmody (*pro hac vice*)
bcarmody@susmangodfrey.com
Shawn J. Rabin (*pro hac vice*)
srabin@susmangodfrey.com
Steven Shepard (*pro hac vice*)
sshepard@susmangodfrey.com
Alexander P. Frawley (*pro hac vice*)
afrawley@susmangodfrey.com
SUSMAN GODFREY L.L.P.
1301 Avenue of the Americas, 32nd Floor
New York, NY 10019
Telephone: (212) 336-8330

John A. Yanchunis (*pro hac vice*)
jyanchunis@forthepeople.com
Ryan J. McGee (*pro hac vice*)
rmcgee@forthepeople.com
MORGAN & MORGAN, P.A.
201 N Franklin Street, 7th Floor
Tampa, FL 33602
Telephone: (813) 223-5505
Facsimile: (813) 222-4736

Michael F. Ram, CA Bar No. 104805
MORGAN & MORGAN
711 Van Ness Ave, Suite 500
San Francisco, CA 94102
Tel: (415) 358-6913
mram@forthepeople.com

Attorneys for Plaintiffs

26